ITEA Journal 2010; 31: 485–494

Net-Ready Key Performance Parameter: A Measurable, Testable, and Operationally Relevant Means of Assessing Joint Interoperability

Danielle M. Koester
Chief, Engineering & Policy Branch,
Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona
Shaina Williams
Command and Control Systems Branch, JITC, Fort Huachuca, Arizona
Kathleen Powers
Senior Systems Engineer,
Northrop Grumman Mission Systems, Fort Huachuca, Arizona
Karen Vincent
Senior Test & Evaluation Engineer,
Northrop Grumman Mission Systems, Fort Huachuca, Arizona

In an effort to overcome community difficulties regarding the testability of the Net-Ready Key Performance Parameter (NR-KPP), the Joint Interoperability Test Command, as the Department of Defense's sole Joint Interoperability Certifier, has established and implemented a detailed approach for defining, testing, and evaluating the NR-KPP consistent with the Chairman of the Joint Chiefs of Staff Instruction 6212.01E. This methodology provides a measurable, testable, and operationally relevant approach to NR-KPP test and evaluation for Joint Interoperability Certification.

Key words: Joint interoperability certification; Joint Interoperability Test Command; test data; DoD architecture framework (DODAF); information exchange, requirements.

The Net-Ready Key Performance Parameter (NR-KPP) was formalized in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01C dated November 20, 2003. Since that time, CJCSI 6212.01 has undergone two major revisions resulting in the current CJCSI 6212.01E dated December 15, 2008 (CJCSI 2008). With each revision, the NR-KPP has grown in size and complexity resulting in both confusion and anxiety for program managers across the Department of Defense (DoD). Arguments have been made that the NR-KPP is neither measurable nor testable. Additionally, it is often viewed as not being operationally relevant. The fact that "Net-Ready" is not a traditional KPP in structure has often been a source of confusion as well. In order for systems in the Department to be secure, interoperable, and able support the mission at hand, it is critical that there is a clear understanding of what the NR-KPP is, how to implement it, and how to test, evaluate, and certify for Joint Interoperability in accordance with the CJCSI 6212.01E.

Interoperability policy and guidance

Governing the Joint Interoperability Certifier role are several policies, the most important of which is Title 10, Section 2223, of the United States Code, which gives the DoD Chief Information Officer (CIO) the responsibility of ensuring interoperability of information technology and national security systems. The certification role has been delegated to Joint Interoperability Test Command (JITC) by the DoD CIO. From a practical standpoint, however, the CJCSI 6212.01E is the instruction that is most referenced with respect to roles and responsibilities for joint interoperability evaluation and certification within the Department. The JITC serves as DoD's sole Joint Interoperability Certifier, in addition to their role

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Net-Ready Key Performance Parameter: A Measurable, Testable, and Operationally Relevant Means of Assessing Joint Interoperability	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Interoperability Test Command (JITC),Fort Huachuca,AZ,85670-2798**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

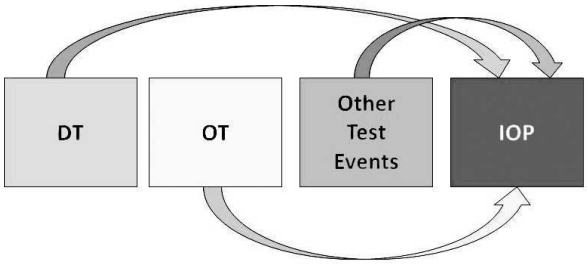

Figure 1. Life cycle test events serve as data points for interoperability certification.

as one of five DoD Operational Test Agencies (OTA). JITC also provides "in the field" support with any interoperability-related issues through the JITC Hotline (1-800-LET-JITC).

Joint Interoperability Test Certification process

In order to issue a Joint Interoperability Test Certification (the proper name for the JITC certification), the interoperability certifier must evaluate a system for compliance with each element of the NR-KPP. The NR-KPP is the evaluation framework used to determine whether or not a system will receive a Joint Interoperability Test Certification *(Figure 1)*. This evaluation uses data collected during developmental testing, operational testing, security testing, demonstrations, exercises, or any other reliable source of test data. The goal is to leverage data and test events to the maximum extent possible, in order to reduce or eliminate the need to conduct separate interoperability testing. For this reason, it is highly recommended that programs involve the interoperability tester early in the life cycle. By being involved early, interoperability testers are able to influence or participate in test events that can be used to collect data for interoperability certification. In the long run, program managers save money by funding the interoperability test agency early, greatly reducing the need for separate interoperability test events.

The Joint Interoperability Test Certification process starts with a Joint Staff certified requirements document. Requirements documents such as Capability Development Documents (CDD), Capability Production Documents (CPD), or Information Support Plans (ISP) are certified by the Joint Staff J-6 for interoperability and supportability. This certification of requirements provides the foundation for issuing the Joint Interoperability Test Certification *(Figure 2)*. Without Joint Staff certified requirements, a Joint Interoperability Test Certification is not possible; although an "assessment" may be given, pending approval of requirements.

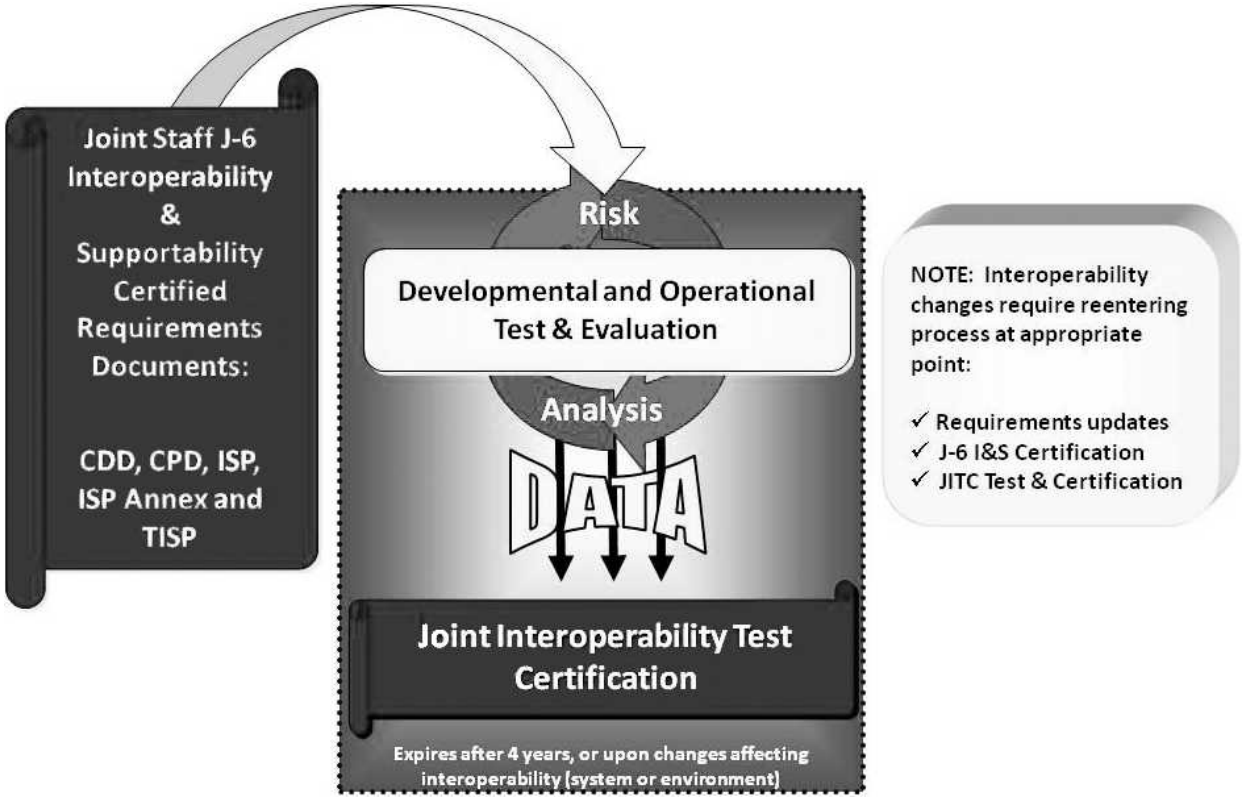

Figure 2. Joint interoperability test certification process.

Table 1. The net-ready key performance parameter.

KPP	Threshold	Objective
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure and operationally effective information exchanges to enable a Net-Centric military capability.	The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.	The capability, system, and/or service must fully support execution of all operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.

Once the system requirements have been analyzed, a risk analysis must be conducted to determine exactly what will be tested to achieve the threshold level of the NR-KPP. This determination is made based upon the requirements that are deemed as "Joint" and "critical" for interoperability. After the risk analysis is complete and data elements for certification identified, data collection begins. If test events are not available for leverage, interoperability testers will need to conduct separate test events. Test data are then analyzed to determine whether or not a system will receive a Joint Interoperability Test Certification.

Requirements analysis

So, is the NR-KPP measurable and testable? What gets measured or tested? And how does that relate to the ability to accomplish the mission? It is important to note that the NR-KPP as a stand-alone item is, in fact, not testable. The reason for this is that the NR-KPP is an *evaluation framework* for joint interoperability and not the actual system-level requirements. The measurable and testable requirements are derived from a system's architecture, generally structured in terms of the DoD Architecture Framework (DODAF). For example, as seen in *Table 1*, the NR-KPP requires that a system be able to support execution of its joint critical operational activities (JCOA); however, it is the system's Operational View-5 (OV-5) that actually defines *what* those JCOAs are. Also important to note is that, while DODAF does prescribe specific content for architectures, it does not prescribe *format*. This is especially important for program's that are operating on limited funding because it allows for reuse of contractor developed system design artifacts, regardless of format.

For interoperability test, evaluation, and certification (TE&C), each system JCOA must be evaluated for

- secure, timely, accurate, complete, and useable information exchanges (operationally effective information exchanges);

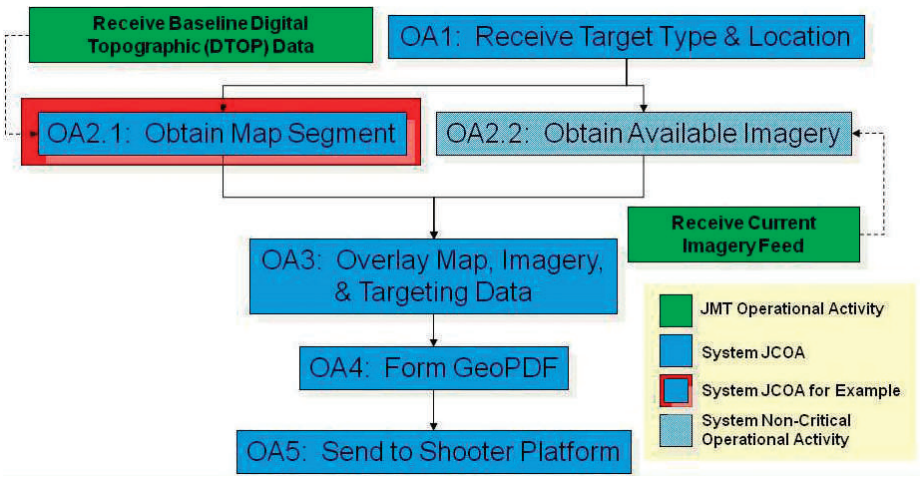

Figure 3. Notional Operational View-5 for Notional Mission Planning Enroute Augmentation System.

- enterprise-level shared data and services that are visible, accessible, understandable, secure, and interoperable (net-centric data and services strategies); and
- standards that have been properly implemented, resulting in no critical deficiencies (Global Information Grid [GIG] Technical Guidance [GTG]).

These are defined as elements 1–3 of the NR-KPP (see *Table 1*).

In addition, the system as a whole must have the information assurance and supportability compliance requirements in place (elements 4–5 in *Table 1*). With respect to information assurance, the system must have completed the requirements for certification & accreditation (C&A), typically through the DoD Information Assurance Certification and Accreditation Process (DIACAP) (although there are other C&A processes that may apply to systems) resulting in interim authority to operate (IATO) (Threshold) or authority to operate (ATO) (Objective). For supportability, the system must ensure that

- any Global Positioning System (GPS) receivers procured are Selective Availability/Anti-Spoofing Module (SAASM) compliant,
- any radio solutions that operate in the Joint Tactical Radio System (JTRS) range are JTRS solutions or that a JTRS waiver has been given by Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]), and
- for spectrum-dependent systems, a Stage 4 DD Form 1494 is in place.

Since information assurance and supportability requirements are relatively static in nature, we will focus on the dynamic requirements defined by NR-KPP elements 1–3 from *Table 1*.

Identify JCOAs

Let us use a fictional example to illustrate this concept. In this fictional example, the Notional Mission Planning Enroute Augmentation System (NMPEAS) is our proposed system under test. Let us also assume that there is an established and accredited joint mission thread (JMT) for mission planning that has been developed by the appropriate operational sponsor. The mission thread defines the activities that must occur to execute mission planning and is tied to the appropriate Universal Joint Tasks to define tasks and metrics for mission accomplishment. The JMT is constructed of various operational activities, two of which are supported by NMPEAS. These operational activities, as shown in *Figure 3*, are

- receive Baseline Digital Topographic (DTOP) data, and
- receive current imagery feed.

The NMPEAS Operational Activity OA2.1: Obtain Map Segment provides a capability that enables "Receive DTOP Data." Simply put, "receive DTOP data" is an activity of the *joint mission thread* (mission planning), and "obtain map segment" is an activity of the *system* that supports the thread activity. There may be a number of system activities that, together, provide the overarching capability defined in the thread. In this example, we will use "obtain map segment" as our representative JCOA for defining measurable and testable criteria for interoperability.

Identify operational information exchange requirements

For our representative JCOA, we must now establish the information exchange requirements (IER) necessary to support execution of that activity,

Needline ID	IER ID	IE Name & ID	Content	Scope	Accuracy	Language	Sending OP Node	Sending OP Activity
NL02 NL03	IER020	IE002: Target Area DTOP	Target area topographic map segment	One or more missions	Resolution 1:25,000	N/A	ON5: Intelligence Cell	**OA2.1 Obtain Map Segment**

Receiving OP Node	Receiving OP Activity	UJTL/ METL	Trans. Type	Trigger Event	Criticality	Periodicity	Timeliness
ON1: Targeting Cell	**OA2.1: Obtain Map Segment**		Automated map segment request/ response	NMPEAS User Request	Critical	As needed	<30 seconds

Figure 4. Notional Mission Planning Enroute Augmentation System Operational View-5 information exchange requirements example.

using the system's OV-3. As shown in *Figure 4*, there is an IER associated with OA2.1 (IER 020), which requires a 30-second "round trip" on a request/response for map data between the intelligence cell and the targeting cell (operational nodes). This is an example of a measurable and testable requirement associated with the NR-KPP. To determine whether or not this IER is "operationally effective" it must take place within a 30-second window, as stated in the operational requirements. Additionally, the data must be complete, accurate, secure, and usable to the warfighter in the conduct of the mission.

Identify system data exchange requirements

At the next level of decomposition, IER 020 is broken out into system data exchanges (SDEs), as defined in the system's SV-6 (see *Figure 5*). This notional example shows a request (SDE021) that must take place within 10 seconds, and a response (SDE022) that must take place within 15 seconds. This supports our operational requirement of a 30-second round-trip time. In addition, the SDE must be able to meet the defined throughput requirements, the data received must be complete, accurate, secure, and usable to the warfighter in the conduct of the mission.

Identify net-centric data and service requirements

Once the data exchanges for evaluation have been identified, the system must be analyzed for use of net-centric data and services. This is important since many systems will be providing data and services to the enterprise for use by other systems. If those data and services are not readily available for consumption, capabilities will be degraded. While the Data/Service Exposure Verification Tracking Sheets are the mandated method of documenting data and services provided to the enterprise, a good system architecture will clearly show what data and services are being

Info Exch ID	System Data Exch ID	System Interface Name/ID	Data Element Name	Content	Format Type	Media Type	Data Standards
IER 020	SDE021	NMPEAS link to enclave LAN	Target area map segment request	Target coord, map segment boundary length	SOAP	Electronic	W3C SOAP v1.2 W3C, XML 1.0 (5th ed) IETF, RFC 2616 1,1 IETF STD 7, 9/91 IETF STD 5, 9/91 IEEE Std 802.3 2008
IER 020	SDE022	DTSS link to enclave LAN	Target area TOPO map segment	TOPO map segment centered on target coord	TFTP	Electronic	MIL-PRF-89037A, 5/99 MIL-STD-2401, 1/94 IETF STD 33, rev 2 IETF STD 7, 9/91 IETF STD 5, 9.91 IEEE Std 802.3 2008

Sending System	Receiving System	Trans. Type	Triggering Event	Criticality	Periodicity	Timeliness	Throughput
NMPEAS	DTSS	Automated request	NMPEAS request "Get Target Area"	C	As needed	<10 s	6 req/min
DTSS	NMPEAS	Automated response	NMPEAS target area map request	C	As needed	<15s	4 resp/min

Figure 5. Notional Mission Planning Enroute Augmentation System SV-6 example.

Table 2. Net-centric data and service requirements for interoperability.

Net-Centric Data Requirements	Net-Centric Service Requirements
Data is Visible Post discovery metadata in an Enterprise Catalog: Department of Defense (DoD) Discovery Metadata Specification (DDMS) conformant discovery metadata is posted in the Net-Centric Enterprise Services (NCES) Enterprise Catalog or other compatible/federated enterprise catalog that is visible to the Enterprise. Use appropriate keywords for discovery: Discovery keywords should reflect common user terms, be appropriate for mission area or data type, be understandable, and conform with MDR requirements that map back to COI identified mission data.	**Services are Visible** Publish a description of the service or access mechanism - Descriptions (metadata) for the service or access mechanism are published in an enterprise service registry, e.g., the NCES Service Registry. Comply with enterprise-specified minimum service discovery requirements - The data access mechanism complies with enterprise-specified minimum service discovery requirements, e.g., a Universal Description, Discovery and Integration (UDDI) description to enable federated discovery.
Data is Accessible Post data to shared space: Data asset is available in a shared space, i.e., a space that is accessible to multiple end users. Provide access policy: If data is not accessible to all users, a written policy on how to gain access is available and accurate. Provide serving (access) mechanism: Shared space provides serving (access) mechanisms for the data. I.e., a service provides users with access to the data. Publish active link to data asset: The Enterprise Catalog DoD Discovery Metadata Specification (DDMS) entry contains an active link (e.g., Uniform Resource Identifier (URI)) to the data asset.	**Services are Accessible** Provide an active link to the service in the enterprise catalog - Active link (e.g., Uniform Resource Identifier (URI)) to the specified service is included in the enterprise catalog metadata entry (i.e., metacard) for the specified service. Provide an active link to the service in the NCES Service Registry - URIs as the operational end points for services shall be registered in the NCES Service Registry by referencing the WSDL (that is in the MDR).
Data is Understandable Publish semantic and structural metadata - Semantic and structural metadata are published in the Enterprise Catalog. Register data artifacts in DoD MDR - XML schema definitions (XSD), eXtensible Markup Language (XML) instances, data models (such as entity relationship diagrams) and other appropriate artifacts are registered in the DoD Metadata Registry (MDR).	**Services are Understandable** Publish a description of the service or access mechanism to the NCES Service Registry - Metadata for the service or access mechanism are published in the NCES Service Registry. Publish service artifacts to DoD MDR - Web Service Description Language (WSDL) documents, and other appropriate artifacts are registered in the DoD Metadata Registry (MDR). Provide service specification or Service Level Agreement (SLA) - A service specification or Service Level Agreement (SLA) exists for services and data access mechanisms.
Data is Interoperable Base vocabularies on Universal Core (UCore) - Semantic vocabularies reuse elements of the Universal Core (Ucore) standard. Comply with COI data-sharing agreements - Semantic and structural metadata conform to interoperability agreements promoted through communities, e.g., Community of Interest (COI). Conform to DDMS - All metadata, including record-level database tagging and in-line document tagging, complies with DDMS.	**Services are Trusted** Operate services in accordance with SLA - The service meets the performance standards in the SLA Include security mechanisms or restrictions in the service specification - The service specification describes security mechanisms or restrictions that apply to the service Enable continuity of operations and disaster recovery for services - The service has a defined and functional Continuity of Operations Plan Provide NetOps Data (NetOps Agility) - Services and data access mechanisms provide operational states, performance, availability, and security data/information to NetOps management services, e.g., Enterprise Management, Content Management, and Network Defense services
Data is Trusted Provide information assurance and security metadata - All metadata, including record-level database tagging and in-line document tagging, includes data pedigree and security metadata, as well as an authoritative source for the data (when appropriate).	**Use of Core Enterprise Services (CES)** - Core Enterprise Services (CES) are used in accordance with DoD CIO mandates

provided. In this example, NMPEAS is not providing any data/services to the enterprise, but since a SOAP request is used in communication with DTSS (see *Figure 5*) there is, more than likely, a Web service being provided by DTSS that provides the requested map information. Clearly, if the DTSS service is not readily available for use, then NMPEAS will not be able to successfully execute IER020. All net-centric data and service assets must comply with the requirements defined in *Table 2*, tailored as necessary in the Joint Staff certified requirements document, in order to be readily available for use across the enterprise.

Identify high-risk standards

Using the JCOAs as a guideline, the system's Technical View-1 (TV-1) is analyzed to determine what standards are implemented that support a JCOA and are high-risk (i.e., military unique, critical to interoperability, etc). *Figure 5* ties the standards to the specific data exchanges that support JCOAs. In this example, perhaps SOAP 1.2 is considered a "high-risk" standard due to known interoperability issues with other Web service standards. The system would be tested for proper implementation of this standard and, ideally, would have a detailed implementation profile

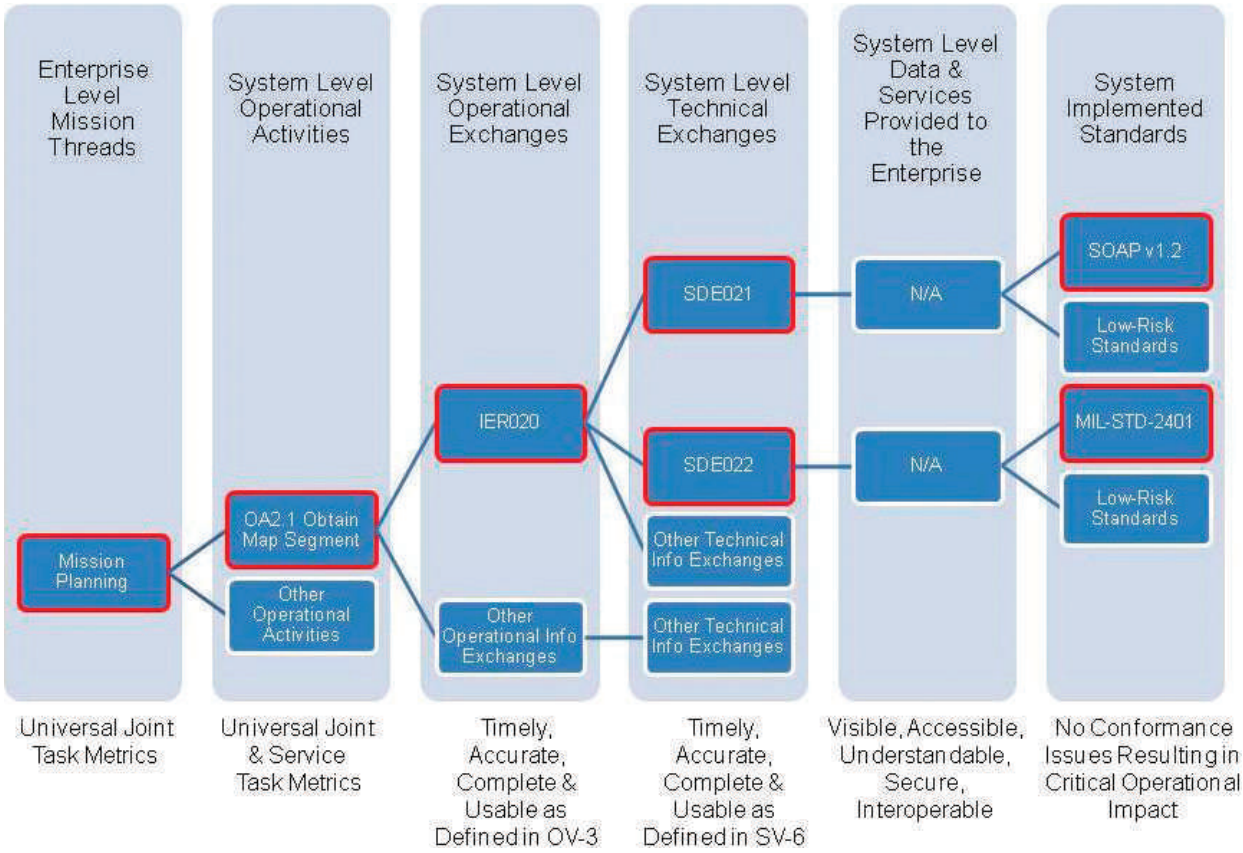

Figure 6. Requirements decomposition into notional test measures for interoperability (Notional Mission Planning Enroute Augmentation System [NMPEAS] Joint Interoperability Certification requirements in red).

that states exactly *how* the standard is being implemented, as is the vision of GIG Technical Profiles.

Document interoperability test criteria

Upon completion of a detailed requirements analysis, test criteria can be easily defined and documented. The goal is to identify these criteria early in the system life cycle, so that program managers can plan for testing, and testers can better plan to leverage each other's events and data. The vision is that testers can test together but evaluate independently to ensure that tester's needs are met and program managers are able to maximize testing return on investment through reuse of test events and test data. These interoperability test criteria, if included in program documentation such as the Test and Evaluation Master Plan (TEMP), will provide the test community and program managers early visibility into interoperability test and certification requirements. A notional breakdown of requirements and measures can be seen in *Figure 6*.

Test, evaluation, and certification

When assessing compliance with the NR-KPP, it is important to test in an operationally realistic environment. This ensures that the results of testing will mirror the system's behavior when fielded in the operational environment. For example, if loading conditions during testing do not represent the conditions of fielding, then test results regarding the timeliness of information exchanges could misrepresent how the system will behave when in the field. This is especially critical when evaluating the first two elements, operationally effective information exchanges and compliance with the Net-Centric Data and Services Strategies. *Table 3* gives high-level information regarding test and reporting for the NR-KPP. Detailed test procedures are available in the JITC NR-KPP Testing Guidebook (DoD 2010).

Upon completion of test and evaluation, a determination is made as to the certification status of the system under test. *Table 4* provides detailed information regarding the different types of interoperability certifications, a description of each, and the fielding recommendation associated with them.

Conclusion

The NR-KPP provides a measurable and testable evaluation framework for joint interoperability test,

Table 3. Net-ready key performance parameter test and evaluation procedures.

NR-KPP Element	Test Procedure	Evaluation
Operationally Effective Information Exchanges	Assess timeliness, accuracy, completeness and usability of information exchanges that support JCOAs in an operationally realistic environment.	System must meet all information exchange requirements that support joint critical (T)/all (O) operational activities.
Net-Centric Data and Services Strategy Compliance	Assess net-centric services and data for visibility, accessibility, understandability, trust and interoperability (VAUTI) IAW JITC NR-KPP Testing Guidebook	System must meet all VAUTI requirements for net-centric data and services that support joint critical (T)/all (O) operational activities.
GIG Technical Guidance	Evaluate system for proper implementation of high-risk standards through conformance testing or reuse of test results from approved organization.	No critical standards conformance-based deficiencies were identified in DT and OT by a combination of government and/or commercial verifications or JITC standards testing or conformance certifications that included all high-risk standards in the TV-1 that support joint critical (T)/all (O) information exchanges.
Information Assurance	Verify system receipt of IATO/ATO, ensure system was tested in approved IA configuration, and as necessary, conduct additional IA scans.	System tested in approved IA configuration, no issues identified during IA scans, and receipt of an IATO (T)/ATO (O).
Supportability	Verify system has met requirements for SAASM, Spectrum and JTRS.	GPS receivers procured are SAASM compliant (T/O) Spectrum dependent system have Stage 4 DD 1494 (T/O) Radios are JTRS solutions or a waiver has been received from ASD(NII) (T/O)

evaluation, and certification. When viewed in the context of joint mission threads and system solution architecture products, it provides a comprehensive means for evaluating joint interoperability that is operationally relevant. A step-by-step process, as shown in *Figure 7*, defines how system solution architectures are easily decomposed into clearly defined test measures providing the test community and program managers the chance to plan for test execution and test data reuse among key stakeholders. While often mistaken as solely a technical requirement or merely a paperwork "compliance" check, the NR-KPP provides the means to tie together technical, system, and operational requirements into meaningful measures. ❑

Ms. Danielle Koester is Chief of JITC's Engineering and Policy Branch within the Strategic Planning and Engineering Division. She has over 10 years of experience in both government and industry focusing on the research, development, engineering, test and evaluation of Information Technology and National Security Systems. Ms. Koester holds a bachelor's degree in mathematics from the College of Saint Elizabeth, Morristown, New Jersey, and a master's degree in systems engineering from Stevens

Table 4. Interoperability certifications as per ''Interoperability and Supportability of Information Technology and National Security Systems'' (CJCSI 6212.01E 2008).

Certification	Description	System can be fielded? (Y/N)
Standards Conformance Certification	System is certified for conformance to a standard/standards profile	No
Joint Interoperability Test Certification	Full system certification. System meets at least all critical interoperability requirements	Yes
Limited Joint Interoperability Test Certification	System meets subset of critical interoperability requirements	Yes, with Interim Certificate to Operate (ICTO)
Interim Joint Interoperability Test Certification	Capability module has adequately demonstrated interoperability for at least all critical threshold requirements identified in the increments	Yes
Special Interoperability Test Certification	Certification is based on J-6 approved requirements other than the NR-KPP, e.g., use of Unified Capability Requirements (UCR) for voice switches	Yes
Non-Certification	Critical operational impacts expected. Provides a warning to the Warfighter.	No
Interoperability Assessment	PM would like to determine interoperability status. System may lack J-6 certified requirements.	No

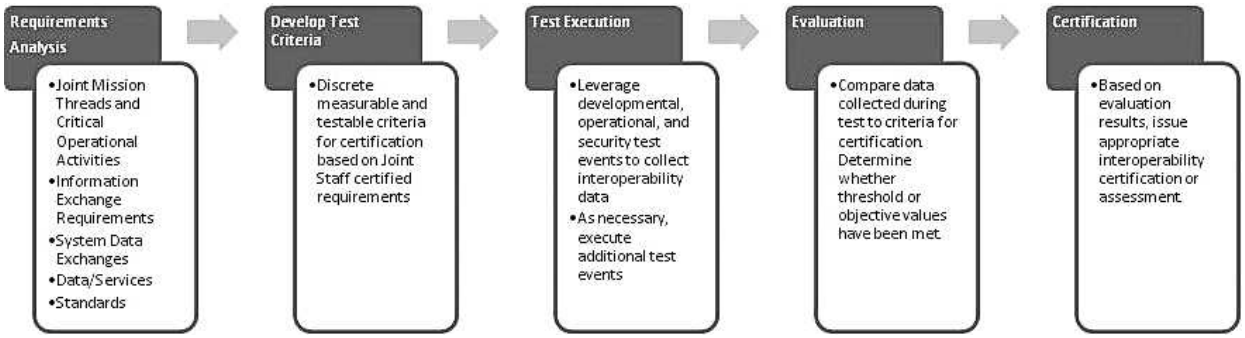

Figure 7. Net-ready key performance parameter test, evaluation, and certification process.

Institute of Technology, Hoboken, New Jersey. Previous assignments include Capability Test Team Lead for the Net-Enabled Command Capability, Project Lead for the Network Enabled Battle Command (NEBC) program, and Information Management Integrated Product Team Lead for the Objective Force Warrior program. A member of the Defense Acquisition Corps, Ms. Koester holds Level III DAWIA certification in Systems Planning, Research, Development and Engineering and Test & Evaluation Engineering. She is the current vice-president of the Huachuca Chapter of the International Test and Evaluation Association.

Shaina Williams is a Test Officer in the Command and Control (C2) Systems Branch within the C2 Battlespace Awareness Portfolio at the Joint Interoperability Test Command. She manages and performs Joint Interoperability Test and Evaluation (T&E) activities that include developing, coordinating, and managing the planning, execution, reporting, budget, and contractor support required to meet the T&E requirements for DoD Information Technology and National Security Systems. Ms. Williams holds a bachelor's degree in computer information systems from Wayland Baptist University and is currently pursuing her master's degree in systems engineering. E-mail: shaina.williams@disa.mil

Ms. Kathleen Powers works for TASC, Inc., as a senior systems engineer supporting JITC's Strategic Planning and Engineering Division. She has 16 years of experience in communications and systems engineering, focusing on signal processing software development as well as T&E processes. Ms. Powers holds a bachelor's degree in electrical engineering from Clarkson University, Potsdam, New York, and a master's degree in electrical engineering from John Hopkins University, Baltimore, Maryland. Ms. Powers is a member of the Institute of Electrical and Electronics Engineers and holds a U.S. patent for a "System for recognizing signal of interest within noise." E-mail: powersk@ieee.org

Ms. Karen Vincent is a Senior Test and Evaluation Engineer working for TASC, Inc., supporting the Joint Interoperability Test Command's Strategic Planning and Engineering Division. Ms. Vincent has more than 25 years as a systems engineer for the acquisition, architecture development, engineering, and testing of command, control, communications, computers, intelligence, surveillance, and reconnaissance systems. Ms. Vincent holds a bachelor of science degree in electrical engineering and computer science engineering from Northern Arizona University. Previous assignments include 3 years as project director for the States U.S. Army Information Systems Engineering Command's Image Product Library Bandwidth Expansion and Engineering Web Development projects, 4 years as North American Air Defense Command/U.S. Space Command Architecture Development project team leader, 2 years as the U.S. Air Force Tactical Data Link Message Standard representative to the Joint and North Atlantic Treaty Organization Data Link Working Groups, and 4 years as Project Manager for the Peacekeeper and Minuteman Ballistic Missile Systems Integration and Electromagnetic Compatibility project. Ms. Vincent is a member of the Defense Acquisition Corps, holding a Level II certification in Acquisition.

References

CJCSI. 15 December 2008. CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems." 20 July 2010. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf (accessed October 18, 2010).

DoD. 2 December 2004. DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense." 1 October 2007. http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf (accessed October 18, 2010).

DoD. 22 June 2010. JITC NR-KPP Testing Guidebook, version 1.0. 20 July 2010. https://www.us.army.mil/suite/doc/23429848 (accessed October 18, 2010).

DoD CIO. 9 May 2003. "Department of Defense Net-Centric Data Strategy." 1 October 2007. http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf (accessed October 18, 2010).

DoD CIO. March 2007. "Department of Defense Net-Centric Services Strategy." 1 October 2007. http://www.jcs.mil/j6/DoD_NetCentricServicesStrategy.pdf.

DoD CIO. 11 April 2008. "Department of Defense Defense Information Enterprise Architecture, Version 1.0." 18 August 2008. http://www.defenselink.mil/cio-nii/cio/diea/products/DIEA1.0-Final.pdf.

Sizemore, Nicky. 23 July 2010. "Use of Architecture Products for Evaluating Info Exchange." JITC Internal Architecture Training Briefing.